UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,799	01/15/2004	Hemant Kumar Jain	INT-102/US	8270

30869   7590   08/07/2007

LUMEN INTELLECTUAL PROPERTY SERVICES, INC.
2345 YALE STREET, 2ND FLOOR
PALO ALTO, CA 94306

EXAMINER
SHAIFER HARRIMAN, DANT B

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
08/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/759,799	JAIN, HEMANT KUMAR
	Examiner	**Art Unit**	
	Dant B. Shaifer - Harriman	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _07/02/2007_.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-3,8-10 and 21_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-3,8-10 and 21_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _15 January 2004_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Specification

1.   The disclosure is objected to because of the following informalities: in paragraph

0094, "Multicast Flood Meter 603" should be "Multicast Flood Meter 604," as indicated

in Figure 6. Appropriate correction is required.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claim(s) 1-3 & 8 – 10 & 21 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Malan et al. (US PGPUB # 2002/0032871) in view of Goldstone (US PGPUB #

2002/01011819).

Malan discloses a method and system for detecting, tracking and blocking denial of

service attacks over a computer networks:

- o   Media access controller (MAC) interface (a controller which is coupled to the

    collector, the controller is constructed and arranged to receive and respond to the

    plurality of signals by tracking attributes related to the one or more data packet

    flow anomalies to at least one source, the controller is further constructed and

    arranged to block the one or more data packet flow anomalies using one or more

    filtering mechanisms executed in close proximity to the at least one source;

filtering mechanisms can include a plurality of filter list entries, such as access

control list entries as well as firewall filter entries, and/or a plurality of rate limiting

entries, Paragraph: 0079, 0073, .0065, the examiner notes that to one or ordinary

skill in the art, a firewall filter entry list, or access control list will have a table of

legitimate IP address to accept and or a list of illegitimate IP addresses that the

firewall isn't to accept.);

o   Classification means for classifying data packets according to layer2, layer3,

layer4 (the collector also includes a buffer, which is adapted to receive and

process the plurality of data statistics to generate at least one record that is

communicated to the profiler, Paragraph: 0067, the examiner notes that to one or

ordinary skill in the art, all packets must contain data (i.e. source/destination

address) and most importantly routing information such as what layers the data

packet must take in order to get to its destination, the collector will collect this

information for packet routing purposes);

o   Meter means for maintaining statistics of attacks, and determining whether a

threshold has been reached (a collector interface adapted to receive a plurality of

data statistics from the computer network and to process the plurality of data

statistics to detect one or more data packet flow anomalies and to generate a

plurality of signals representing the one or more data packet flow anomalies

Paragraph: 0066, 0084, 0065);

o Decision multiplexer able to receive decisions from meter means, and capable of informing the Media access controller (MAC) interface of a single decision regarding the data packet statistics (the profiler also includes a database for storing a plurality of data packet flow profiles and related information; a detector is adapted to receive and process the predetermined threshold and the at least one record to detect if attributes associated with the record exceed the predetermined threshold, which represents the one or more data packet flow anomalies, Paragraph: 0084, the examiner notes that the profiler is the multiplexer and the MAC is the zone controller or local controller);

o A source tracking mechanism that multiplicatively incrementing the count for sources that send identified flood data, thereby distinguishing sources from others that send non-flood data (the controller is constructed and arranged to receive and respond to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source, the controller is further constructed and arranged to block the one or more data packet flow anomalies using one or more filtering mechanisms executed in close proximity to the at least one source; filtering mechanisms can include a plurality of filter list entries, such as access control list entries as well as firewall filter entries, and/or a plurality of rate limiting entries Paragraph: 0079, 0073, 0065, the examiner notes that the controller is able to keep track of the various sources that may

send flood data or non-flood data through the profiler and collector utilizes, as

they keep track of the statistic associated with the plurality of data packets

received by the network resources (i.e. computer or server));

o   A SYN flood detection and prevention mechanism have a support means for

creating a plurality of legitimate IP addresses during normal operation when the

TCP state transitions to Established, where the SYN flood detection and

prevention mechanism allows only the plurality of legitimate IP address to be

stored during normal operation (the controller is further constructed and arranged

to block the one or more data packet flow anomalies using one or more filtering

mechanisms executed in close proximity to the at least one source; filtering

mechanisms can include a plurality of filter list entries, such as access control list

entries as well as firewall filter entries, and/or a plurality of rate limiting entries,

Paragraph: 0079, 0073, 0065, the examiner notes that to one or ordinary skill in

the art, a firewall filter entry list, or access control list will have a table of

legitimate IP address to accept and or a list of illegitimate IP addresses that the

firewall isn't to accept);

o   A means for determining a threshold for said connections based on baseline

traffic learned during normal operation (a profiler processes the record to

generate a predetermined threshold which communicates to the detector

(Paragraph: 0068), the profiler also includes a database for storing a plurality of

data packet flow profiles and related information; a detector is adapted to receive

and process the predetermined threshold and the at least one record to detect if

attributes associated with the record exceed the predetermined threshold, which

represents the one or more data packet flow anomalies Paragraph: 0084);

- o Detection of a SYN flood Dos attacks (Paragraph: 0084, the examiner notes that

   the storm detector is able to recognize a SYN flood DOS attack based on

   comparing whether or note a threshold with respect to SYN packet has been

   exceeded.);

- o The rate based denial of service attacks are to an end node or from said end

   node to other end nodes on the internet (The system for detecting, tracking,

   blocking of DOS occurs from one computer to another computer on different

   computer networks, Paragraph: 0057);

- o Receiving packets from a network (The system for detecting, tracking, blocking of

   DOS occurs from one computer to another computer on different computer

   networks, Paragraph: 0057);

- o Creating and storing a table of legitimate IP addresses during normal operation

   when a TCP state transitions to established (Paragraph: 0079, 0080, the

   examiner notes that the controller is able to look at other network resources and

   or routing configurations (i.e. IP addresses of incoming data), and compile or

create a list of legitimate address or illegitimate addresses, that will be used to

filter out malicious variants of DOS attacks.) furthermore, (the controller also

includes a includes a correlator which is used to generate an anomaly table

including the attributes related to the one or more data packet flow anomalies

Paragraph: 0074, 0086, the examiner notes that to one of ordinary skill in the art,

the most common way to track a malicious data packet is by identifying the data

packets source address);

o   Detecting a SYN flood state (Paragraph: 0084, the examiner notes that the storm

detector is able to recognize a SYN flood DOS attack based on comparing

whether or not a threshold with respect to SYN packet has been exceeded);

Malan fails to teach a:

o   zombie flood detection and prevention mechanism having a means for limiting

connections said plurality of legitimate IP addresses stored during normal

operation;

o   An ager means capable of timing out flood states identified by classification

means or meter means, and ager is able to continuously learn, monitor and

update statistics;

However, Goldstone discloses a conventional approach to preventing DOS (denial of service) attacks:

- o Detection of a Zombie flood (The attacking client's DOS event is initiated when an otherwise legitimate client IP address that has been spoofed by a attacking client, initiates a connection to a network server multiple times to cause congestion to the server or network, this multitude of connection attempts to connect to the server causes congestion or a flood which in fact is a Zombie flood. Zombie floods are caused by clients who initiate connection to the internet multiple times with a legitimate IP address that will not be blocked by the security entities (i.e. routers, firewalls) of the network or internet, the multiple connection request to the network server causes congestion or a flood, which will not allow other users of the network to request connection through that particular server to logon to the internet until a the timing session for each request to logon to the internet, times out (Paragraph: 0045, 0046, 0050);

- o An ager for timing out of a flooding event (Zombie floods are caused by clients who initiate connection to the internet multiple times with a legitimate IP address that will not be blocked by the security entities (i.e. routers, firewalls) of the network or internet, the multiple connection request to the network server causes congestion or a flood, which will not allow other users of the network to request connection through that particular server to logon to the internet until a the timing

session for each request to logon to the internet, times out (Paragraph: 0045,

0046, 0050);

Malan and Goldstone are analogous art because they are from the "same field of

endeavor," which is the field of detecting, tracking, blocking or preventing "denial of

service attacks," or data packet floods moreover, specifically SYN (Synchronization)

floods, and Zombie floods.

At the time of the invention, it would have been obvious to one of ordinary skill in the art,

having the teachings of Malan and Goldstone before him or her, to modify the detection,

tracking, blocking, of a DOS attacks of Malan to include the prevention of a Zombie

flood DOS attack of Goldstone, because it would allow for more efficient security

coverage or protection of a network, if the DOS attack on the target server or network is

initiated from spoofed legitimate address instead of a known illegitimate attacker

address.

The suggestion/motivation for doing so would have been to enabled a network that

contains security entities (i.e. routers, firewalls), to detect, track, block viruses (i.e.

zombie flood attacks) that come from legitimate IP addresses that would otherwise be

authorized access to the internet through the target server an continue in attacking the

network through multiple internet access requests; to detect a zombie like flood

originating from a spoofed legitimate address, Paragraph: 0056 of Malan and

Paragraph: 0038 of Goldstone.

Therefore it would have been obvious to combine Goldstone with Malan to obtain the

invention as specified in the instant claim(s).

Response to Arguments

1.   On page 9 of the specification, the label "308" for the "Control and Statistics

Block" is corrected to read "314" as indicated in Figure 3.

The examiner has verified the applicants changes to the specification and

accepts the changes to the specification and that no new matter has been added.

2.   On page 18 of the specification, the reference to "Multicast Meter 604" is

corrected to read "Multicast Flood Meter 604" as indicated in Figure 6.

The examiner has verified the applicants changes to the specification and

accepts the changes to the specification and that no new matter has been added.

3.   On page 20 of the specification, the reference to "Multicast Flood Meter 603" is

corrected to read   "Multicast Flood Meter 604" as indicated in Figure 6.

The examiner was unable to verify the applicant's changes to the specification

and doesn't accept the applicants remark that the specification has been

changed to reflect the necessary. The examiner finds the applicants remark

concerning this manner moot. Please see the disclosure objection above, under

the heading specification.

4.   Claims 1 and 8-10 are amended. Claims 4-7 and 11-20 are cancelled. New claim
        21 is added.

The examiner has verified that claims 1 and 8-10 are amended, and that claims

4-7 and 11-20 are cancelled and new claim 21 is added, the examiner accepts

these amendments.

5.   Regarding the specification, the Office objected to three minor informalities in the

disclosure. In response, Applicant amends the specification to address all the

informalities pointed out in the Action.

The examiner has verified the applicants changes to the specification and

accepts the changes to the specification and that no new matter has been added.

6.   Claims 8-10 and 18-20 were rejected under 35 USC 112 because the term

"network characteristic" was considered vague and indefinite. Applicant responds

by amending the claims to remove the term "network characteristics." The new

language in the claims is supported in various portions of the specification, e.g.,

page 9, lines 6-17; page 29, lines 1-5 and 15-20; and page 31, lines 15-26.

The examiner has verified the applicant's changes to claims 8 – 10 and 18 – 20

and accepts the changes to claims 8 – 10 and 18 – 20   and that no new matter

has been added.

7.   Claims 1-9 and 12-20 were rejected under 35 USC 112 because it was unclear to

the examiner whether the limitations of the claims were directed toward machine

parts or software. Applicant responds by pointing out that the recited limitations

are clearly physical components of a tangibly realized computing apparatus (e.g.,

the MAC interface recited in claim 1). Regarding various other limitations of claim

1, it is noted that computational components of a computing apparatus may be

implemented not only as software but also in firmware or in hardware.

Irrespective of the particular implementation of a given computational

component, its physical realization in the computing apparatus constitutes a part

of a computing apparatus or system, and is recited as such in the present claims.

Such physical components may be characterized in terms of their functions.

Thus, the physical components recited in the claims are not mere limitations to

software but are rather limitations characterizing tangible components of the

claimed computing apparatus or system.

The examiner has verified the applicant's claim that a MAC interface can be

hardware or software or firmware. The examiner with reference to claims 1 –9

and 12 – 20, accepts the reasoning and logic to claims 1 –9 and 12 – 20 and that

no new matter has been added.

8.   Claims 1-10 and 11-20 were rejected under 35 USC 101 because the claims

allegedly do not fall within a statutory category. In particular, the Office states in

the Action that "each limitation of the claims is drawn towards software per se",

and that "the claims are, at best, functional descriptive material per se." Applicant

respectfully disagrees. Claim 1 is directed toward a digital computing apparatus

and explicitly recites various physical components of such. For example, the first

limitation of claim 1 recites a media access controller (MAC) interface, which is a

physical component, and the second limitation recites a classification means

operatively coupled to the MAC interface. These limitations are clearly physical in

nature and cannot be accurately or fairly characterized as "software per se" or

"functional descriptive material per se." Accordingly, Applicant respectfully

requests withdrawal of the rejection as being based on an incorrect reading of

the claim language.

The examiner has verified the applicant's claim that a media access controller

(MAC) interface can be hardware or software or firmware, is therefore considered

a manufacturer, which clearly is 35 U.S.C. 101 compliant. The examiner with

reference to claims 1 –10 and 11 – 20, accepts the reasoning and logic to claims

1 –10 and 11 – 20 and that no new matter has been added.

9.   Claims 1-3 & 8-10 & 21 are all rejected under 35 U.S.C. 103a, as being obvious.

Claims 1-3 & 8-10 & 21 are being rejected behind as being unpatentable over

Malan et al. (US PGPUB # 2002/0032871) in view of Goldstone (US PGPUB #

2002/01011819). Please see the 35 U.S.C. 103a rejection above for further

explanation.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

D.S.H.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER